ATTI

DELLA

REALE ACCADEMIA DEI LINCEI

ANNO CCCIII.

1906

SERIE QUINTA

RENDICONTI

Classe di scienze fisiche, matematiche e naturali.

VOLUME XV.

1° Semestre.

ROMA

TIPOGRAFIA DELLA R. ACCADEMIA DEI LINCEI

PROPRIETÀ DEL CAV. V. SALVIUCCI

1906

Matematica. — *Théorie et construction de tables permettant de trouver rapidement les facteurs premiers d'un nombre.* Nota di ERNEST LEBON, presentata dal Socio V. VOLTERRA.

En m'appuyant sur des propriétés non encore signalées de certaines progressions arithmétiques, je suis arrivé à construire des tables donnant *très rapidement* la solution du double problème suivant:

Un nombre étant donné, reconnaître s'il est premier ou composé, et, dans le second cas, trouver ses facteurs premiers.

Le procédé que j'emploie est applicable à de grands nombres.

Mon Mémoire sur ce sujet a été signalé à l'Académie des Sciences de Paris, dans la séance du 3 juillet 1905 (1).

1. Soient B le produit $\alpha\beta...\lambda$ de nombres premiers consécutifs $\alpha, \beta, ..., \lambda$, à partir de 2; P le produit $(\alpha - 1)(\beta - 1)...(\lambda - 1)$; I l'un quelconque des P nombres premiers à B et inférieurs à B; K un nombre successivement égal aux entiers positifs, à partir de 0.

On reconnaît aisément que: *Chacun des systèmes des* P *progressions arithmétiques de terme général* $BK + I$ *renferme tous les nombres premiers autres que ceux qui forment* B.

On peut dire que B est la *base* du système considéré et que I est l'*indicateur* d'un terme de ce système.

Deux indicateurs sont dits *complémentaires* lorsque leur somme est égale à la base.

2. Soient N, D et M des nombres d'un système de progressions de base B. Pour éviter l'ambigüité dans les explications, j'écrirai ainsi: $BK' + I'$ la forme du diviseur D.

Il est évident que *le nombre* N *est ou non divisible par le diviseur* D *selon que* K *et* M *sont ou non tels que l'équation*

$$(a) \qquad BK + I = MD$$

soit satisfaite, B, I *et* D *étant connus.*

3. Soient k et m les valeurs *minima* de K et M satisfaisant à l'équation (a) et n un nombre successivement égal aux entiers positifs, à partir de 0. L'égalité

$$K = k + nD$$

(1) Comptes Rendus, Tome CXLI, n. 1, Paris, 1905, in 4°, pag. 78.

donne la valeur de K à laquelle correspondent tous les nombres N divisibles par le diviseur D.

De cette égalité, on tire la formule

$$n = \frac{K - k}{D}, \tag{1}$$

où K est le quotient entier obtenu en divisant N par B; le reste de cette division est la valeur de I.

On voit que: *Selon que la valeur trouvée pour* n, *en appliquant la formule* (1), *est entière ou fractionnaire, le nombre* N *est ou non multiple du diviseur* D.

Donc *la Table des nombres* k *établie pour un système de base* B *permet de reconnaître si* N *est premier, en divisant* K *par les nombres premiers inférieurs à* $\sqrt{N}$, *à partir de* λ, *et, si* N *n'est pas premier, de trouver ses facteurs premiers.*

On conçoit que cette méthode est d'autant plus expéditive que la base B est plus grande.

Avant d'appliquer la formule (1), il ne faut pas oublier que, si l'on considère un nombre N', on doit d'abord, pour avoir N, enlever de N' les facteurs premiers de la base B.

4. J'appellerai *caractéristiques* les nombres k.

5. Pour trouver méthodiquement et rapidement les caractéristiques k qui correspondent aux P progressions arithmétiques d'un système de base B, on peut se servir de la formule suivante, obtenue après avoir remplacé, dans l'équation (a), K et M par k et m, D par sa forme:

$$k = \frac{I'm - I}{B} + K'm. \tag{2}$$

La formule (2) donne la caractéristique k quand la valeur de m est telle que le binôme $I'm - I$ soit divisible par B.

6. Les trois théorèmes suivants, faciles à démontrer, permettent de réduire notablement les opérations pour le calcul des caractéristiques k.

I. *Au produit* $I'm$ *des deux indicateurs* I' *et* m *correspondent un indicateur* I *et une caractéristique* k; *cette caractéristique* k *convient aux deux diviseurs* I' *et* m *du nombre* $I'm$ *de la progression arithmétique de base* B *et d'indicateur* I *donné par ce produit.*

II. *Les* P *progressions arithmétiques d'un système de base* B *étant rangées dans l'ordre croissant des indicateurs* I *de leurs termes, la somme des deux caractéristiques* k *et celle des deux valeurs de* m, *relatives à*

un même diviseur D *et à deux progressions équidistantes des extrêmes, sont respectivement égales à* D — 1 *et à* B.

III. *Si les valeurs de* I, *de* k_I, *de* I′ *et de m sont telles que l'égalité*

$$Bk_I + I = I'm$$

existe, et si l'on considère l'équation

$$Bk_{B-I} + (B - I) = (B - I')\,m,$$

où les deux indicateurs B — I *et* B — I′ *sont complémentaires des deux indicateurs* I *et* I′ *de l'égalité précédente, la caractéristique inconnue* k_{B-I} *est donnée par la formule*

$$k_{B-I} = m - 1 - k_I.$$

7. D'après les théorèmes II et III, il suffit, pour calculer le binôme I′*m* — I, d'associer à la première moitié des P valeurs de I′ la première moitié des P valeurs de *m*, rangées dans l'ordre croissant.

Le reste obtenu en divisant I′*m* par B est l'indicateur I relatif à une progression du système de base B.

Quand K′ est nul, le premier terme de la formule (2) donne, dans chacune des P progressions du système de base B, les P caractéristiques *k* correspondant aux P valeurs de I′.

D'après le théorème I, comme les caractéristiques *k* correspondant à l'indicateur I sont les mêmes quand D égale soit I′, soit *m*, il suffit de commencer les produits I′*m* à partir de la valeur de *m* égale à la valeur considérée de I′, c'est-à-dire au carré de I′. On sait que l'on applique le premier terme de la formule (2) seulement aux valeurs de *m* qui égalent les $\frac{P}{2}$ premiers indicateurs. D'ailleurs, aux produits de 1 par les indicateurs correspondent des caractéristiques *k* évidemment égales à 0. Par suite, parmi les P^2 caractéristiques *k* relatives aux P diviseurs qui égalent les indicateurs, il y a au plus $\frac{P(P-2)}{8}$ caractéristiques *k* dont la détermination exige une multiplication et une division.

8. La Table de caractéristiques *k* relatives à la base 30030, avec les diviseurs premiers de 17 à 30029 permet de résoudre le problème en question entre 1 et 30030^2 ou 901800900, c'est-à-dire pour des nombres beaucoup plus grands que le nombre 8999999 auquel s'arrêtent les Tables imprimées de facteurs premiers des nombres. Elle a de plus l'avantage de donner souvent plus d'un des facteurs premiers du nombre considéré, sans obliger à faire des divisions.

Soit N un nombre de la forme 30030K + I. Pour faire les essais, on s'arrêtera au diviseur premier D_n immédiatement inférieur à $\sqrt{N}$.

Si l'on ne trouve aucune différence $K - k$ divisible par les diviseurs premiers de 17 à D_n, N est premier.

Si l'on arrive à une différence $K - k$ divisible par le diviseur premier D, inférieur à D_n, N admet ce diviseur premier D. On divise N par D, le quotient obtenu par D, etc. Soit N_1 le dernier quotient ainsi obtenu: on opère avec N_1 comme on vient d'opérer avec N, en commençant par le diviseur premier qui suit D et on trouve que N_1 égale le produit de caractéristiques ou que N_1 est premier.

On reconnaît si une différence $K - k$ est divisible par le diviseur D correspondant le plus souvent sans effecteur la division par D de cette différence.

Pour reconnaître *instantanément* si une différence $K - k$ est divisible par le diviseur D correspondant, il suffit d'avoir, en même temps que la Table des caractéristiques relatives à la base 30030 jusqu'au diviseur 30029, une Table des restes R obtenus en divisant par les diviseurs D les nombres entiers consécutifs de 17 à 30029: en effet, une différence $K - k$ est divisible par le diviseur D correspondant, lorsque les valeurs de R et de k qui correspondent à ce diviseur sont égales.

La nouvelle Table occuperait une surface au moins 10 fois plus petite que celle qui serait occupée par les Tables qui existent et celles que l'on construirait jusqu'à 901800900, en adoptant l'ancienne disposition.

Fisica. — *Influenza degli orli sulla capacità elettrostatica di un condensatore* (1). Nota del dott. R. Magini, presentata dal Corrispondente A. Battelli.

1. Nelle precedenti Note su questo stesso argomento ho esaminato le formole principali da usarsi per la correzione della capacità dipendentemente dalla perturbazione provocata dall'orlo nella distribuzione elettrica di un condensatore. In questa mi propongo di sviluppare un artificio, già indicato nel principio del presente lavoro, che potrà permettere di isolare e di mettere in maggiore evidenza l'influenza dell'orlo, specialmente nel caso in cui venga usato l'anello di guardia, che riduce quell'influenza così notevolmente da farla quasi scomparire di fronte alla capacità del condensatore e da impedire una verifica diretta e rigorosa. D'altra parte, mi sono anche proposto di darne una conferma sperimentale, e di fare un esame sommario delle formole studiate sin qui per tre soli valori della distanza, per vedere se esse sono delle semplici astrazioni o seppure trovano una qualche rispondenza sperimentale.

(1) Lavoro eseguito nell'Istituto di Fisica della R. Università di Pisa.